In the Specification:

Please amend the specification beginning on Page 11, line 31 through page 12, line 8 as follows:

Figure ~~5~~ 5A is a diagram illustrating the structure of messages in accordance with the dynamic host configuration protocol (DHCP);

Figure ~~5A~~ 5B is a diagram illustrating the structure of the encapsulated vendor-specific extensions field in accordance with DHCP;

Figure ~~5B~~ 5C is a diagram illustrating the structure of vendor-specific information in accordance with one embodiment of the invention;

Figure 6 is a diagram of a DHCP server and a DHCP client for exchanging configuration information in accordance with one embodiment of the invention; and

Figure 7 is a flowchart illustrating the input and use of the vendor-specific information of Figure ~~5B~~ 5C in accordance with one embodiment of the invention.

Please amend the specification beginning on Page 18, line 15 through line 23 as follows:

Figure ~~5~~ 5A illustrates the structure of a response 500 from the DHCP server back to a DHCP client. The response incorporates a Code field 510, a Length field 511 and a Value field 512. The Code field 510 is a one-byte field for which there is a predefined set of values to identify the contents of the corresponding Value segment 512. For example, if Code=6, the Value portion 512 comprises one or more addresses of a DNS server. The Length portion 511 is then a multiple of 4, depending upon the number of addresses included in the message (since IP uses 4-byte addresses). Similarly, if Code=3, then the Value segment 512 lists the IP addresses for routers on the client's subnet.

Please amend the specification beginning on Page 20, line 4 through line 32 as follows:

RFC 2132 recommends that if more than one item of information is incorporated into the Value field corresponding to Code=43, then this should be done by using encapsulated vendor-

specific options having a structure such as that shown in Figure 5A (which mirrors the standard DHCP structure of Figure ~~5~~ 5A). Thus the recommended format of the encapsulated vendor-specific information 500A comprises Code field 510A, Length field 511A, and Value field 512A. Note that all of information 500A is then incorporated into the Value field 512 of a DHCP response having Code 510 =43.

However, there are two drawbacks with a direct implementation of the structure of Figure ~~5A~~ 5B. Firstly, the size of the Code field limits the number of configuration items that can be defined. Assuming a 1-byte Code field, with no predetermined special values, there is a maximum of 256 available Code values. Whilst this number is probably sufficient for most situations, it is desirable to avoid having such a fixed maximum. Secondly, some of the configuration data to be transmitted to the DHCP client may be sensitive from a security perspective, for example, relating to passwords, or accessing information from an LDAP server.

Accordingly, one embodiment of the invention adopts the structure shown in Figure ~~5B~~ 5C to encode the vendor-specific information 500A. (As with Figure ~~5A~~ 5B, the block 500A corresponds to the contents of the Value field 512 associated with Code 510 =43 for a DHCP response 500). Again, there is a triplet formation, which can nominally be regarded as corresponding to the Code, Length and Value fields of response 500 (and also 500A). However, in this case, the third field 512B (nominally the Value field) is used to hold one or more name-value pairs, while the first field 510B (nominally the Code field) is used to store an indicator of encryption applied to the third field 512B. The second field 511B of Figure ~~5B~~ 5C is used to store a length indicator, as for Figures ~~5 and 5A~~ 5A and 5B. (Accordingly, the second field 511B is largely conventional, and will not be discussed herein in detail).

Please amend the specification beginning on Page 21, line 23 through line 28 as follows:

The Value field may be (partly) encrypted in order to preserve the security of any sensitive information that it contains. The Code field 512B is then used to specify the form of encryption applied to the Value field 512B. This maintains the self-defining nature of message

500A, and exploits the fact that since the name of the parameter is now included in the (nominal) Value field 512B, the (nominal) Code field 510B is freed up for some other task (compared to the arrangement of Figure ~~5~~ 5A).

Please amend the specification beginning on Page 23, line 11 through line 17 as follows:

Although the vendor-specific configuration information stored in the DHCP repository 600 adopts at least in part the structure of Figure ~~5B~~ 5C (rather than the structure of Figure ~~5A~~ 5B of existing systems), it will be noted that this change in the contents of repository 600 is transparent to the DHCP server 412 (and to the repository 600 itself). Hence the DHCP server 412, including repository 600, may be implemented using an existing system without modification to the DHCP server 412 itself, thereby providing compatibility with current systems and networks.

Please amend the specification beginning on Page 23, line 28 through Page 24, line 4 as follows:

In accordance with one embodiment of the present invention, configuration utility 624 includes an encrypt/decrypt unit 626. This allows a user to encrypt selected parameters of the vendor-specific configuration information, when these are initially being specified by a system administrator. The encrypt/decrypt unit 626 is also responsible for then setting the corresponding Code field 510B to the appropriate value to indicate this encryption (as discussed above in relation to Figure ~~5B~~ 5C). Conversely, when configuration information is downloaded from DHCP repository 600, the encrypt/decrypt unit 626 is able to parse the DHCP information, and perform any necessary decryption on this data, as specified by Code field 510B.

Please amend the specification beginning on Page 24, line 15 through line 24 as follows:

Figure 7 illustrates a flowchart showing how the configuration data for a DHCP client 620 may be set in accordance with one embodiment of the invention. The method begins with a system

administrator or manager entering configuration data for the client 620 (step 710), for example by using the configuration utility 624. The vendor-specific portion of this data, corresponding to Code field 510 =43, is provided as a set of name-value pairs, as depicted in Figure ~~5B~~ 5C. Next a determination is made to see if any of these name-value pairs are to be encrypted (step 720). In some cases there may be a default encryption setting for certain parameters (according to their name values), or alternatively this may be entirely at the discretion of the system administrator entering the data.